ABSTRACT

We consider one-round games between a classical referee and two players. One of the main questions in this area is the parallel repetition question: Is there a way to decrease the maximum winning probability of a game without increasing the number of rounds or the number of players? Classically, efforts to resolve this question, open for many years, have culminated in Raz’s celebrated parallel repetition theorem on one hand, and in efficient product testers for PCPs on the other.

In the case where players share entanglement, the only previously known results are for special cases of games, and are based on techniques that seem inherently limited. Here we show for the first time that the maximum success probability of entangled games can be reduced through parallel repetition, provided it was not initially 1. Our proof is inspired by a seminal result of Feige and Kilian in the context of classical two-prover one-round interactive proofs. One of the main components in our proof is an orthogonalization lemma for operators, which might be of independent interest.

Categories and Subject Descriptors

F.1.3 [Theory of Computation]: Computation by Abstract Devices—Complexity Measures and Classes

General Terms

Theory

Keywords

Entangled games, parallel repetition

1. INTRODUCTION

Two-player games play a major role both in theoretical computer science, where they have led to many breakthroughs such as the discovery of tight inapproximability results for some constraint satisfaction problems, and in quantum physics, where they first arose in the context of Bell inequalities, which give a path towards experimentally testing the nonlocality of Quantum Mechanics. In such games, a referee (or verifier) chooses a pair of questions from some distribution and sends one question to each of two non-communicating players (or provers), who then respond with answers taken from some finite set. The referee, based on the questions and answers, decides whether to accept (i.e., whether the players win). The main question of interest is the following: given the referee’s behavior as specified by the game, what is the maximum winning probability achievable by the players? Somewhat surprisingly, the answer to this question turns out to depend on whether we force the players to behave classically, or allow them to use quantum mechanics. In the former case, the players’ answers are simply deterministic functions of their inputs\(^1\), and the maximum probability of winning is known as the classical value of the game. In the latter case the players, though still space-time separated, may perform any physical operation allowed by Quantum Mechanics. In particular, they may start the game in an arbitrary entangled state, and each perform arbitrary measurements on their share of the state upon receiving their respective questions. The maximum winning probability in this case is known as the entangled value of the game. This model of entangled players (also known as that of non-local games) dates back at least to the work of Tsirelson, and it has been intensely studied in recent years; yet many questions about it are still wide open.

One of the most important and interesting questions in this context is the parallel repetition question. It is well known that one can reduce both the value and the entangled value of a game by repeating it sequentially, or alternatively, by repeating it in parallel with several independent pairs of players. However, for many applications (like hardness of approximation results or amplifications preserving zero-knowledge) we need a way to decrease the winning probability without increasing the number of rounds or the

\(^1\)One can allow the players to use randomness, but this does not change their maximum winning probability.
number of players, i.e., while staying in the model of two-
player one-round games. Parallel repetition, a method first
introduced in [13], is designed to do just that: in its most ba-
sic form, in the $\ell$-parallel repeated game, the referee simply
chooses $\ell$ pairs of questions independently and sends to each
player his corresponding $\ell$-tuple of questions. Each player
then replies with an $\ell$-tuple of answers, which are accepted
if and only if each of the $\ell$ answer pairs would have been
accepted in the original game.

Clearly the value of an $\ell$-parallel repeated game is at least
the $\ell$-th power of the value of the original game, since the players
can just answer each of the $\ell$ questions independently
as in the original protocol. However, contrary to what intu-
tion might suggest and to the case of sequential repetition,
parallel repetition does not necessarily decrease the value of
a game in a straightforward exponential manner\footnote{See [9] for a classical example, and [5] for an example using entangled players due to Watrous. See also [20] for another example where parallel repetition does not reduce the value of a game at the exact rate one would expect if the players were playing independently.}. The par-
allel repetition question is that of finding upper bounds on the
value of a repeated game, and for a long time no such upper
bound, even very weak, could be proved. First results
date to Verbitsky [29] who showed that indeed the value
goes to zero with the number of repetitions. Following this,
Feige and Kilian [10] showed that the value decreases poly-
nomially with the number of repetitions for the special case
of so-called projection games (in which the second player’s
answer is uniquely determined by the first player’s). They
used a modified parallel repetition procedure in which a large
fraction of the repetitions are made of dummy rounds, that is,
rounds in which the questions are chosen independently
at random for both players, and in which any answer is
accepted. In this paper we deviate somewhat from the com-
mon terminology, and use the term “parallel repetition” even
when referring to such more general procedures. Finally, in
a breakthrough result, Raz [25] showed that the value of
a game repeated in parallel indeed decreases exponentially
with the number of repetitions (albeit not exactly at the
same rate as sequential repetition). There is still very ac-
tive research in this area, mostly on simplifying the analysis,
which, over a decade later, remains quite involved, and
improving it for certain special cases of games [15, 24, 11, 26,
2, 3, 1, 27].

1.1 Previous work

In this paper we focus on parallel repetition of games
with entangled players. The only two previous results in
this area are for two special classes of games. First, Cleve
et al. showed that for the class of XOR games (i.e., games
with binary answers in which the referee’s decision is based
solely on the XOR of the two answers), perfect parallel rep-
etition holds [5]. This means that the entangled value of
an $\ell$-parallel repeated game is exactly the $\ell$-th power of
the entangled value of the original game. Parallel repetition has
also been shown to hold for the more general (but still quite
restricted) class of unique games [21] (i.e., games where the
referee applies some permutation to the answers of the sec-
ond player and accepts if and only they match those from
the first player). One might also add a third result by Holen-
stein [15], who proved a parallel repetition theorem for the
so-called no-signaling value; since the no-signaling value is
an upper bound on the entangled value, this can sometimes
be used to upper bound the entangled value of repeated
games. However, there is in general no guarantee regarding
the quality of this upper bound, and in many cases (e.g., all
unique games) the no-signaling value is always 1, making it
useless as an upper bound on the entangled value.

It is important to note that in these results the entan-
gled value of the parallel repeated game is never analyzed
directly; instead, one uses a “proxy” such as a semidefinite
program [5, 21] or the no-signaling value [15], whose behav-
ior under parallel repetition is well understood. Moreover,
in all these cases, the proxy’s value is efficiently computable.
This unfortunately gives a very strong indication that such
techniques cannot be extended to deal with general games.
Indeed, it is known that it is NP-hard to tell if the entan-
gled value of a given game is 1 or not [19, 18]; hence, unless
P=NP, for any efficiently computable upper bound on the
entangled value, there are necessarily games whose entan-
gled value is strictly less than 1 yet for which that upper
bound is 1 (and such games can often be exhibited explicit-
ly without relying on P≠NP). We note that some of the
early parallel repetition results for the classical value [12]
followed the same route (of upper bounding the value by a
semidefinite program) and were limited to special classes of
games for the exact same reason.

To summarize, no parallel repetition result (not even one
with very slow decay) is known for the entangled value of
general games, and, moreover, the known techniques are un-
likely to extend to this case. Hence the natural question:

Can parallel repetition decrease the entangled value
of games? If so, can we bound the rate of de-
crease?

In parallel to work on the parallel repetition problem, the
related question of product testing arose in the context of
error amplification for PCPs [8, 6, 16, 17]. Roughly speak-
ing, the question here is to design tests by which a referee
can check that the players play according to a product strat-
ey, i.e., answer each question independently of the other
questions (as one would expect from an honest behavior).
Note that if the players are constrained to follow a prod-
uct strategy, then their maximum winning probability must
necessarily go down exponentially, hence the connection to
the parallel repetition question. The result of Feige and Kil-
ian [10] mentioned above in fact also shows that the strat-
ey of the players must have some product structure, and
recently there has been lots of renewed interest in this ques-
tion leading to much stronger product testers [7]. In the
case of entangled players, however, absolutely nothing was
known:

Is there a way to test if the strategy of entan-
gled players is in some sense close to a product
strategy?

1.2 Our results

In this work we answer both questions in the affirmative,
and our main result can be stated as follows.

Theorem 1 (informal). For any $s < 1$, $\delta > 0$, and
entangled game $G$, there is a corresponding $\ell$-parallel re-
peated game $G'$, where $\ell = \text{poly}(s^{-1}, \delta^{-1})$, such that if
the value of $G$ is less than $s$ then the value of $G'$ is at most $\delta$, whereas if the value of $G$ is 1 then this also holds\(^3\) for the repeated game.

The dependency of $\ell$ on $\delta$ in our theorem is polynomial, whereas as we already mentioned it is known that in some cases this dependence can be made poly-logarithmic (and this is certainly the case if the players are assumed to play independently). While a poly-logarithmic dependence is important in some applications for which one would like to perform amplification up to an exponentially small value, in many cases the main use of parallel repetition is to amplify a small “gap” between value 1 and value $s = 1 - \frac{1}{\text{poly}(|G|)}$ to a constant gap, say between 1 and 1/2. In this case the polynomial dependence of $\ell$ on $(1 - s)^{-1}$ that we obtain is optimal (up to the exact value of the exponent).

The informal statement above hides some details, which we now discuss. The kind of parallel repetition we perform depends on the structure of the game $G$, and we distinguish whether it is a projection game or not.

**Repetition for projection games.**

If $G$ is a projection game, then the repeated game is obtained by independently playing the original $G$ on a subset of the repetitions, and playing dummy rounds in the other repetitions. We note that projection games form a wide class of games that captures most of the games one typically encounters in the classical literature (see [24]).

If, in addition, the game happens to be a free game (i.e., a game in which the referee’s distribution on question pairs is a product distribution), then the dummy questions are no longer needed and hence our analysis applies to the standard $\ell$-fold repetition.

**Repetition for general games.**

If the game $G$ does not have the projection property, then it is necessary to add a number of consistency rounds to the repetition. In those rounds the referee sends identical questions to the players, and expects identical answers. As before, the other rounds of the repetition are either the same game $G$ or dummy rounds. The consistency questions are added to play the role of the projection constraints.

This kind of repetition raises the following issue\(^4\): namely, it is not obvious that honest entangled players can answer the consistency questions correctly. This implies that, even if the original game had value 1, players might not be able to succeed in the consistency questions and hence the value of the repeated game might not equal 1 anymore. This may or may not be an issue depending on where the original game comes from. In many cases it is known that, if there is a perfect strategy, either it does not require any entanglement at all, or it can be achieved using the maximally entangled state. In both cases it is not hard to see that players will be able to answer consistency questions perfectly, and hence our result holds. Because of this we regard this issue as a minor one; however it might be important in some contexts.

### 1.3 Proof idea and techniques

We focus on the case of projection games, as the proof of the other cases does not present additional challenges.

\(^3\) See the discussion following the theorem for some caveats.

\(^4\) This is why we treat the projection case separately, despite it leading to similar decay.

The starting point of our proof is the work of Feige and Kilian [10], for which the following intuition can be given. Our goal as the referee is to force the players to use a product strategy, preventing any elaborate cheating strategies. In other words, we want to make sure that the player chooses his answer to the $i$th question based only on that question and not on any of the other $\ell - 1$ questions. Towards this end, the referee chooses a certain (typically large) fraction of the $\ell$ question pairs to be independently distributed dummy questions, the answers to which are ignored. These dummy questions are meant to confuse the players: if they were indeed trying to carefully choose their answer to a certain question by looking at many other questions, now most of these other questions will be completely random and uncorrelated with the other player’s questions, so that such a strategy cannot possibly be helpful.

In more detail, Feige and Kilian prove the following dichotomy theorem on the structure of single-player repeated strategies (that is, maps from $\ell$-tuples of questions to $\ell$-tuples of answers): either the strategy looks rather random (in which case the players cannot win the game with good probability — this is where the projection property is used) or it is almost a serial or product strategy, i.e., the answer to each question is chosen based on that question only (in which case the player is playing the rounds independently, and his success probability will suffer accordingly).

Our proof follows a similar structure. However, an important challenge immediately surfaces: the proof in [10], and indeed all proofs of parallel repetition theorems or direct product tests, make the important initial step of assuming that the player’s strategies are deterministic (which is easily seen to hold without loss of generality for the case of classical players). And indeed, it is not at all trivial to extend those proofs to even the randomized setting without making this initial simplifying assumption. To give a simple example, an important notion in Feige and Kilian’s proof is that of a dead question — simply put, a question to which the player does not give any majority answer, when one goes over all possible ways of completing that specific question into a tuple of questions for the repeated game. It is easily seen that, in the case of a deterministic strategy, dead questions are harmful, as the players are unlikely to satisfy the projection property on them. However, it is just as easily seen that for many randomized strategies, good or bad, all questions are dead.

This illustrates the kinds of difficulties that one encounters while trying to show parallel repetition in the case of entangled players, when one cannot simply “fix the randomness”. The issue we just raised is not too hard to solve, and others are more challenging. Indeed the main difficulty is to define a proper notion of almost serial for operators, which would in particular incorporate the inherent randomness of quantum strategies. It turns out that the right notion is the notion of consecutive measurements (rather than tensor products of measurements for each question, a tempting but excessively strong possibility). Based on a quantum analogue of Feige and Kilian’s dichotomy theorem, we are able to show that the almost serial condition induces a condition of almost orthogonality on the player’s operators. At this point we need to prove a genuinely quantum lemma, which lets us extract a product strategy from the almost-orthogonal con-

\(^5\) We refer to Ryan O’Donnell’s excellent lecture notes [23, 22] for a helpful exposition of Feige and Kilian’s proof.
dation. This novel orthogonalization lemma is at the heart of our proof. We obtain that the players approximately perform a series of consecutive measurements, each depending only on the current question. An upper bound on the value of the repeated game then follows.

**Organization of the paper.**

We start with a few definitions, including a description of the form of the repeated games that we consider, in Section 2. We then give a detailed overview of the structure of the proof of our main result in Section 3. Due to lack of space most proofs could not be included, but are available in the online technical report arXiv:1012.4728. Finally, Section 4 contains a discussion of our result on approximate joint block-diagonalization of positive matrices which are close to being orthogonal.

## 2. PRELIMINARIES

### 2.1 Games

In this paper we study two-player one-round games. Let $Q$ and $A$ be finite sets. An entangled game (or simply game) can be defined as follows.

**Definition 2.** An entangled game $G = (V, \pi)$ is given by a function $V: A^2 \times Q^2 \rightarrow \{0,1\}$ and a distribution $\pi: Q^2 \rightarrow [0,1]$. The referee samples questions $(q', q)$ according to $\pi$, and sends $q'$ to the first player and $q$ to the second player. He receives back answers $a'$, respectively. He accepts those answers if and only if $V(a', a | q', q) = 1$. The value of the game is

$$\omega^*(G) = \sup_{|\Psi\rangle, A_H, B_H} \sum_{(q', q) \in Q^2} \sum_{(a', a) \in A^2} \pi(q', q) V(a', a | q', q)$$

where the supremum is taken over all finite-dimensional Hilbert spaces $H$, all a priori shared states $|\Psi\rangle \in H$ and all Projective Operator-Valued Measurements (POVMs)$^6$ $A'_H = \{A'_H\}_{a \in A}$ and $B_H = \{B_H\}_{a \in A}$ on $H$.

We note that by standard purification techniques (see [4]) one can assume that for each question $q$ each player performs a projective measurement with outcomes in $A$ (i.e., $\sum_{a \in A} A'_H = I_d$ and $(A'_H)^I = A'_H = (A_H)^I$).

We will be interested in some special classes of games.

**Definition 3.** A game $G = (V, \pi)$ is called a

- **Projection game** if for every $q', q \in Q$ and $a' \in A$, there is a unique $a \in A$ such that $V(a', a | q', q) = 1$.
- **Free game** if $\pi = \pi_A \times \pi_B$ is a product distribution.
- **Symmetric game** if $\pi$ is symmetric, and for any $q', q, a, a'$ we have $V(a', a | q', q) = V(a, a' | q, q')$.

### 2.2 Repeated games

We consider two different types of repeated games. The first one, originally used by Feige and Kilian, applies to projection games, and we describe it in Definition 4. The second type of repetition applies to consistency games, and is closer to the direct product testing technique originally introduced by Dinur and Reingold [8]; we explain it in Definition 5.

**Definition 4 (Feige-Kilian repetition).** Let $\ell$ be any integer, and define $C_1 := \ell^{1/8}$ and $C_2 := \ell - C_1$. Given a two-player projection game $G = (\pi, V, Q, A)$, its $\ell$-th Feige-Kilian repetition is the following game $G_{FK}(\ell)$:

- The referee picks a random partition $[\ell] = M \cup F$, where $|M| = C_1$ and $|F| = C_2 = \ell - C_1$. Indices in $M$ will be called “game” indices, while indices in $F$ will be called “confuse” indices.
- The referee picks $(q_M, q_M') \sim c_1 (Q \times Q)^{C_1}$.
- He picks $(q_F, q_F') \sim (\pi_A \times \pi_Q)^{C_2} (Q \times Q)^{C_2}$, where $\pi_A$ is the marginal of $\pi$ on the first player, and $\pi_B$ the marginal on the second player.
- The referee sends the questions to the players (without specifying which questions are of which type). On game questions he verifies that the original game constraint is satisfied. He accepts any answers to confuse questions.

**Definition 5 (Dinur-Reingold repetition).** Let $\ell$ be any integer, and define $C_1 := \ell^{1/8}$, $C_1 = 2C_1$ and $C_2 := \ell - C_1$. Given a two-player symmetric game $G = (\pi, V, Q, A)$, its $\ell$-th Dinur-Reingold repetition is the following game $G_{DR}(\ell)$:

- The referee picks a random partition $[\ell] = R \cup G \cup F$, where $|R| = C_1$, $|G| = C_1$, and $|F| = C_2$. Indices in $R$ will be called “consistency” indices, those in $G$ will be called “game” indices, and those in $F$ “confuse” indices.
- The referee picks $C_1$ questions $q_R \sim c_1 (Q \times Q)^{C_1}$ and sets $q_R = q_R$, where $\pi_A$ is the marginal of $\pi$ on the first player (since we assumed $G$ was symmetric, this is the same as $\pi_B$, the marginal on the second player).
- The referee picks $C_1'$ pairs of questions $(q_G, q_G') \sim (\pi_A \times \pi_Q)^{C_2} (Q \times Q)^{C_2}$.
- He picks $(q_F, q_F') \sim (\pi_A \times \pi_Q)^{C_2} (Q \times Q)^{C_2}$.
- The referee sends the questions to the players (without specifying which questions are of which type). On consistency questions he verifies that both answers, from Alice and from Bob, are identical. On game questions he verifies that the original game constraint is satisfied. He accepts any answers to confuse questions.

Note that, if a game $G$ has value 1, then its Dinur-Reingold repetition does not necessarily also have value 1, as the player’s optimal strategy in $G$ might not be consistent. A consistent strategy is one in which whenever the players are asked the same question they provide the same answer with certainty. This may not always hold of an optimal strategy; nevertheless the following lemma shows that we can assume it holds in some natural settings.

**Lemma 6 (Lemmata 3 and 4 in [19]).** Let $G = (V, \pi)$ be an arbitrary 2-player entangled game. Then there exists a game $G' = (V', \pi')$ of the same classical and quantum values
with twice as many questions, and such that $\pi'$ and $V'$ are symmetric under permutation of the variables. Moreover, given any strategy $P_1, \ldots, P_N$ with entangled state $|\Psi\rangle$ that wins $G$ with probability $p$, there exists a strategy $P'_1, \ldots, P'_N$ with entangled $|\Psi'\rangle$ that wins $G'$ with probability $p$ and is such that $P'_1 = \cdots = P'_k$ and $|\Psi'\rangle$ is symmetric with respect to the provers $1, \ldots, k$. In addition, if $|\Psi\rangle$ was a maximally entangled state then $|\Psi'\rangle$ is also.

This lemma shows that, if $G$ is any game, then we may symmetrize it and assume that optimal provers are playing according to a symmetric strategy. In particular, if $G$ had value 1, and the optimal strategy used either no entanglement or a maximally entangled state, then this also holds of the optimal strategy in the symmetrized game. Such a strategy is automatically consistent.

2.3 Notation

We introduce some important notation pertaining to repeated strategies, i.e. prover strategies in a repeated game. For every $q \in Q'$, let $\{X^q_{\rho}\}_{\rho \in A'}$ be an arbitrary projective measurement in $d$ dimensions, that is, the $X^q_{\rho}$ are projector matrices, and for any fixed $q$ they sum to the identity over $a$. The position of the questions (or answers) in a tuple will always be fixed and usually clear from the context; for example when we write $q = (q_a, q')$, where $G, F \subseteq [\ell]$ are sets of indices, it is not necessary that the questions $q_a$ are placed before the questions $q_F$ in the tuple $q$; rather their position is determined by the indices in $G, F$. When precision is needed we shall write $(i, q_i)$ to express the fact that question $q_i$ is destined to appear in the $i$-th position of some tuple $q$. We also write $q_{\cdots}$ to denote $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_{\ell}$.

We will consider marginalized POVMs over certain sets $T \subseteq S \subseteq [\ell]$. Given questions $q_S$ indexed by $S$, the marginalized POVM on $T$ is the POVM indexed by answers $a_T$, which results from applying $\{X^{a_T}_{q_S}\}_{a_T}$ for any $q \in Q^{[\ell] \setminus S}$, and ignoring the answers $a$ not in $T$. For any $\rho \geq 0$, the post-measurement state resulting from applying this measurement on $\rho$ is

$$E_{q \in Q^{[\ell] \setminus S}} \left[ \sum_{a \in A^{[\ell] \setminus T}} X^{a_T}_{q_S} \rho X^{a_T}_{q_S} \right]$$

Here the expectation on $q \in Q^{[\ell] \setminus S}$ is taken according to a fixed underlying product distribution $\pi'^{[\ell] \setminus S}$, which will always correspond to the marginal distribution from the original game that is being repeated. In general it will be convenient to define a marginalized operator

$$X^{a_T}_{q_S} := E_{q \in Q^{[\ell] \setminus S}} \left[ \sum_{a \in A^{[\ell] \setminus T}} X^{a_T}_{q_S} \right]$$

This definition satisfies that the probability of obtaining answers $a_T$ when performing the marginalized POVM with questions $q_S$ on any state $\rho$ is exactly $Tr(X^{a_T}_{q_S} \rho)$. Even though our results all hold for general states $\rho$, in this extended abstract we will mostly discuss the simplified case where $\rho = d^{-1} I_d$ is the totally mixed state of arbitrary dimension $d$. In this case, for any $d$-dimensional matrix $A$ we will write

$$Tr_F(A) := d^{-1} Tr(A) = Tr(A \cdot d^{-1} I_d)$$

3. PROOF OVERVIEW

We give a formal account of our results in the next section, before proceeding to give an overview of their proof in Section 3.2.

3.1 Results

We first state our main theorems. They refer to the two types of repetition of an entangled game $G$ defined in the previous section, its $\ell$-th Feige-Kilian repetition $G_{FK(\ell)}$, and its $\ell$-th Dinur-Reingold repetition $G_{DR(\ell)}$. Both types of repeated games are made of $\ell$ independent rounds, played in parallel. Some of these rounds consist of independent repetitions of $G$, while others are either confuse or consistency rounds, containing simple tests independent of the original game (except for the distribution with which questions are chosen in those rounds). Our first result pertains to projection games.

**Theorem 7.** There exists a constant $c \geq 1$ such that, for all $s < 1$ and $\delta > 0$ there is a $\ell = O((\delta^{-1} (1-s)^{-1}))$ such that, if $G$ is a projection game with value $\omega(G) \leq s$, then the entangled value of the game $G_{FK(\ell)}$ is at most $\delta$. Moreover, if the value of $G$ is 1 then the value of $G_{FK(\ell)}$ is also 1.

In the case of free projection games, questions to the players are chosen independently, so that the distribution on questions in the confuse rounds of the game $G_{FK(\ell)}$ is exactly the same as that in the original game. The only difference is that in such a round, all answers are accepted, which can only help the players. Hence the direct parallel repetition of $G$ has a smaller value than its Feige-Kilian repetition, which implies the following.

**Corollary 8.** Let $s < 1$ and $\delta > 0$. Then there is a $\ell = O((\delta^{-1} (1-s)^{-1}))$ such that, if $G$ is a free projection game such that $\omega(G) \leq s$, then the (direct) $\ell$-fold parallel repetition of $G$ has value at most $\delta$.

Our second result is more general, as it applies to arbitrary games. It only comes with the mild caveat that, in order to preserve the fact that the original game had value 1 (whenever this indeed holds), it is required that in that case there also exists a perfect strategy which is consistent.

**Theorem 9.** There exists a constant $c \geq 1$ such that, for all $s < 1$ and $\delta > 0$ there is a $\ell = O((\delta^{-1} (1-s)^{-1}))$ such that, if $G$ is an arbitrary game with value $\omega(G) \leq s$, then the entangled value of the game $G_{DR(\ell)}$ is at most $\delta$. Moreover, if $G$ has a perfect consistent strategy then the value of $G_{DR(\ell)}$ is also 1.

Lemma 6 shows that the requirement that $G$ has a perfect consistent strategy (which is only a requirement in cases where we are interested in preserving the fact that $G$ might have value 1) is satisfied for many examples of games, including those for which we know a priori that, if the value of $G$ is 1, then there is an optimal strategy that either does not use any entanglement at all, or uses the maximally entangled state.

3.2 Proof overview

In the remainder of this section we describe the main ideas behind the proof of Theorem 7 and Theorem 9; full details can be found in the technical report arXiv:1012.4728. In
order to simplify the exposition we make an important assumption: the entangled state shared by the players in the repeated game is the maximally entangled state (of arbitrary dimension $d$). This will allow us to state simplified variants of our main claims, while still preserving the main ideas. Fully general claims and proofs can be found in the technical report available online.

Our goal is to understand repeated quantum strategies, that is, maps $q \in Q'\to \{X^a_q\}_{a\in A'}$ which map tuples of questions $q = (q_1, \ldots, q_\ell)$ to projective measurements $\{X^a_q\}_{a\in A'}$ in dimension $d$. The semantics are that, on receiving questions $q$, a player measures his share of the entangled state $|\Psi\rangle = d^{-1/2} \sum_i |ii\rangle$ according to $\{X^a_q\}_{a\in A'}$, resulting in him sending back answer $a$ with probability $\langle \Psi I_d \otimes X^a_q | \Psi \rangle$. Interestingly, most of the proof will be directly concerned with the measurements $\{X^a_q\}_{a\in A'}$ themselves (together with the reduced density $\rho = \text{Tr}_A |\Psi\rangle \langle\Psi| = d^{-1} I_d$), without reference to the other player’s measurements or even the underlying game.

We will be interested in a strategy’s marginals, as defined in Section 2.3. Given that $X$ was a projective measurement, the marginalized strategy over some subsets $T \subseteq S \subseteq \ell$ is a POVM — it is not necessarily projective any more. Our main results will pertain to the structure of such marginalized strategies. We will show that they are either very random (this is formally called dead later on, and morally means that the marginalized strategy is very far from a projective measurement; rather its singular values tend to be small and spread out), or highly structured (this is formally called serial measurement; rather its singular values tend to be small and spread out), or highly structured (this is formally called serial measurement; rather its singular values tend to be small and spread out), or highly structured (this is formally called serial measurement; rather its singular values tend to be small and spread out), or highly structured (this is formally called serial measurement; rather its singular values tend to be small and spread out). The attentive reader might already see that once this is proven it will be possible to bound the success probability of both types of strategies in the repeated game; however we should warn that the exact statements, and their proofs, are rather technical and carry only a fair share of the intuition we have just given.

We proceed to give a more detailed overview of the structure of the proof of our results. It can be divided into three main steps. The first two steps establish facts about the structure of repeated single-player strategies, and are independent of the game being played, as well as of the other player’s strategy.

**Step 1: A quantum dichotomy theorem.**

In the first step we prove an analogue of Feige and Kilian’s dichotomy theorem [10]. We first make the following definition.

**Definition 10.** Given a strategy $X^a_q$ and a fixed set of questions $q_R$ in positions $R \subseteq \ell$, define the collision probability of $X$ on $q_R$ as

$$P_{\text{col}}(q_R|X) := \sum_{a_R} P_{\text{col}}(q_R, a_R|X)$$

where

$$P_{\text{col}}(q_R, a_R|X) := \text{Tr}_F \left( (X^{a_R}_R)^2 \right)$$

Note that this last expression is just the normalized squared Frobenius norm $d^{-1}\|X^{a_R}_R\|_F^2$. Expression (1) can be interpreted in two different ways. From an operational point of view, it corresponds to the probability that one obtains twice the same answers when one sequentially performs a measurement using the marginalized POVM with elements $\{X^q_{a_R}\}_{a_R}$. In this sense, $P_{\text{col}}$ is a measure of the predictability of the strategy $X^a_q$, pick two completions $q, q'$ at random and measure using first $\{X^q_{a_R}\}_{a_R}$ and then using $\{X^{q'}_{a_R}\}_{a_R}$: $P_{\text{col}}(q_R|X, \rho)$ is the probability of getting twice the same result $a_R$ (while ignoring the other answers $a, a'$). The analytic interpretation is that this is a measure of the entropy of the spectrum of $X^{a_R}_R$, which is maximized when $X^{a_R}_R$ is a projector (for a fixed value of the trace).

The following lets us make the distinction between the two different types of strategies alluded to above.

**Definition 11.** We will say that:

- A block $(R, q_R)$ is $\varepsilon$-dead if $P_{\text{col}}(q_R|X) \leq \varepsilon$. If a block is not $\varepsilon$-dead it is $\varepsilon$-alive. Moreover, we say that the answer $a_R$ is $\varepsilon$-alive if it satisfies

$$P_{\text{col}}(q_R, a_R|X) \geq \varepsilon \text{Tr}_F \left( X^{a_R}_R \right)$$

Note that any $\varepsilon$-alive block has at least one $\varepsilon$-alive answer. Sometimes we will simply say that a block or an answer are alive or dead, leaving the parameter $\varepsilon$ implicit.

- A block $(R, q_R, a_R)$ is $(1-\eta)$-serial if $a_R$ is alive and the following holds:

$$E_{(q_R, a_R)} \left[ P_{\text{col}}(q_R, q_R, a_R|X) \right] \geq (1-\eta) P_{\text{col}}(q_R|X)$$

**Lemma 12.** Assume that $\varepsilon, \eta > 0$ are chosen such that $\eta^3 > 16 C_1^{-1/2}$. Then one of the following holds

1. At least a $(1-\varepsilon)$ fraction of blocks $(R, q_R)$ are $\varepsilon$-dead.
2. At least an $\varepsilon$ fraction of blocks $(R, q_R)$ are $\varepsilon$-alive, and moreover if $(R, q_R)$ is an $\varepsilon$-alive block then

$$\sum_{a_R \text{\- alive but not } (1-\eta)\text{-serial}} \text{Tr}_F \left( X^{a_R}_R \right) \leq \varepsilon/2$$

i.e. alive answers which are not $(1-\eta)$-serial have a small probability of occurring.

**Proof.** We extend the definition of the collision probability to measuring collisions over answers which are not necessarily on the same indices as the questions:

$$P_{\text{col}}(q|X) := \sum_{a_R} \text{Tr}_F \left( (X^{a_R}_R)^2 \right)$$

where now $q$ can be any subset of fixed questions, and $R$ denotes the subset of answers on which we are measuring the collision probability.

**Claim 13.** There exists an integer $1 \leq r^* \leq C_1$ such that

$$E_{R, q_R} \left[ P_{\text{col}}(q_R|X, \rho) \right] - E_{R, q_R, 1, \{i\}} \left[ P_{\text{col}}(q_R, q_R|R \cup \{i\}, X) \right] \leq 8 C_1^{-1/2}$$

where the expectation is taken over all subsets $R$ of size $|R| = r^*$.

$^7$Recall that $C_1, C_2$ are chosen so that $C_1 + C_2 = \ell$: see Definitions 4 and 5 for more details.
Proof. There is a similar statement in [10], and we omit the
detail proof. It is based on Claim 20, which is crucial in
showing that strategies that have been marginalized over
a large number of questions do not depend much on a single
additional random question.

Towards a contradiction, assume the negation of both 1.
and 2. With probability at least $\varepsilon$ a random block $(R,q_R)$ is alive, and moreover if $(R,q_R)$ is alive then alive answers
which are not $(1-\eta)$-serial have a significant contribution.
Fix such an answer $a_R$. Since (3) is not satisfied, summing
over all $a_R$ which are alive but not $(1-\eta)$-serial one can see that the collision probability, for this $(R,q_R)$, must decrease by at least

$$\eta \cdot \sum_{a_R \in R \text{ alive but } (q_R,a_R) \text{ is not } (1-\eta)\text{-serial}} P_{\text{col}}(q_R,a_R|X)$$

By the negation of (4) and the fact that the answers are alive, this quantity is at least $\eta^2/2$. Finally, taking the expectation over the choice of $(R,q_R)$ gives a total decrease in $P_{\text{col}}$ of at least $\eta^2/2$, contradicting Claim 13 if $\eta^2/2 > 8C_\varepsilon^{-1/2}$.

Fleshing out the consequences of this lemma to eventually
show that, in the second case, one can extract a product form
for strategies requires some work, and is the object of the
second step of the proof.

Step 2: A product theorem for serial strategies.

While for a classical deterministic player a serial strategy,
as defined in the previous section, is one which decides on the
answer $a_i$ to most questions $q_i$ not in $R$ as a function of
that question alone, in the quantum setting this is much less
clear. The first task is to decide on what one expects from a
serial strategy. For instance, one might ask for the measure-
ments to take some “approximately-tensor” form; however
we find that this is too strong a requirement. Instead, we first
show that the serial property implies that the player’s measure-
ment operator $\{X_{a_R|q_R}\}_{(q_R,a_R) \in A_R \times I}$ (possibly depending on $q_R$ and $a_R$) that, with probability at least $(1-2\eta^2/4)$ over the choice
of $(i,q_i)$,

$$\sum_{a_i} T_F((X_{q_i|a_i}^R - \Pi_{q_i|a_i}^R)^2) \leq O(\eta^2 \varepsilon/c_2) T_F(X_{q_i|a_i}^R)$$ (5)

where $c_2 > 0$ is a universal constant.

We omit the proof of the claim. The main idea is to express
the $(1-\eta)$-serial condition (3) as an approximate
orthogonality (with respect to the normalized trace inner-
product) between the $X_{q_i|a_i}^R$ and $X_{q_i|a_i'}^R$ for $a_i \neq a_i'$, and then to use the orthogonalization lemma, Lemma 19, in or-
der to extract an approximate block-diagonal structure from
this almost-orthogonality.

Through repeated application of Claim 20 it is not hard to
extend the approximation in Claim 14 to a small number
of additional questions $q_1,\ldots,q_g$, showing that the corre-
sponding measurement also has a block-diagonal form, this
time described by the product of the corresponding projec-
tors $\Pi_{q_i}^R \cdots \Pi_{q_1}^R$. We state the end result below.

Lemma 15. Let $\eta \geq C_\varepsilon^{-1/2}$ and suppose that $(q_R,a_R)$ is
$(1-\eta)$-serial, let $1 \leq q \leq C_\varepsilon^{-2}$ be a fixed factor, and
$(G,q_G)$ chosen at random under the constraint that $G \cap R = \emptyset$ and $|G| = g$. Then with probability at least $(1-2\eta^2/4 - e^{-2\varepsilon})$ over the choice of $(G,q_G)$, there is a partition $G = G' \cup G''$, where $g'' = |G''| \geq (1-4\eta^2/4) g$, such that

$$\sum_{a_{G''}} T_F((X_{a_{G''}|q_{G''}}^R - \Pi_{a_{G''}|q_{G''}}^R)^2)$$

$$\leq O(\eta^2 \varepsilon^2 (1+\varepsilon) T_F(X_{a_R}^R))$$ (6)

Note that, in this lemma, the second term
$$\Pi_{a_{G''}}^R \cdots \Pi_{q_i}^R X_{a_R|q_R}^R \Pi_{q_i}^R \cdots \Pi_{a_{G''}}^R$$
depends on the specific answer $a_{G''}$ only through the pro-
jectors $\Pi_{a_{G''}}^R$. As such, Lemma 15 can be understood as a form of direct product test. Indeed, we will see in the last
step of the proof that dead strategies must fail the repeated
game with high probability. Hence any strategy which has a
non-negligible success in the repeated game must be $(1-\eta)$-
serial for a non-negligible fraction of question-answer pairs
$(qa,aq)$, which by the lemma induces a product form on a
subset of the answers in the other rounds.\(^8\)

Step 3: Both dead and serial strategies fail the repeated
game.

In the last step of the proof we show that both types of
strategies, dead or serial, must fail in the repeated game with
high probability (provided the value of the original game
was bounded away from 1). For the case of dead strategies
this is fairly intuitive: since a dead strategy does not assign
consistent answers to a certain subset of the questions $q_R$, this
implies that the player’s answers in positions $R$ will very
much depend on the questions present in those indices not
in $R$; not only that but it will be virtually impossible for the
other player to correlate well with this player’s answers
on those indices. Here we crucially use the “projection”,
or “consistency” rounds of the repeated game in order to
show that such strategies will fail in those rounds with high
probability. We show the following.

Claim 16. Let $\varepsilon > 0$ be such that $\varepsilon \geq C_\varepsilon^{-1}$, and sup-
pose that $(R,q_R)$ is an $\varepsilon$-dead block. Then the success prob-
ability of the players, conditioned on the referee picking ques-
tions $(q',q)$ such that $q$ includes $q_R$ in the positions in $R$, is
at most $\sqrt{2\varepsilon}$.

The case of serial strategies is slightly harder to analyze, and
it is based on the fact that the block-diagonal form described
in Lemma 15 implies that we can see one of the
players as making a sequential measurement governed by
the $\Pi_{q_i}^R$. Since in this case the player’s answer to question $q_i$
is decided by applying a projective measurement depending
on $q$, alone, in case the original game had a value $s < 1$
\(^8\)We should caution here that the more general claim, valid
also in case $|\Phi|$ is not the maximally entangled state, in-
volves some technical complications; we refer to the techni-
cal version for more details.
such a strategy will fail in at least a fraction \( s/2 \) of the “game” rounds with high probability, and be caught by the referee provided there are enough such rounds. We show the following:

Claim 17. Fix \((R,q_R,a_R)\), and for every \((i,q_i)\), where \(i \in \{0,1\}\) and \(q_i \in Q\), let \(\{\Pi_{g_i}^{q_i}\}_{g_i \in A}\) be a fixed projective measurement. Suppose that Bob’s strategy is such that, with probability at least \(1 - \delta\) over the choice of \((G,q_G)\) and \(G_{1} \subseteq G\) of size \(|G_1| = g\), there is a partition \(G_1 = G'' \cup G'''\) such that \(g'' = |G''| \geq (1 - \delta)q\) and Bob’s POVM satisfies that for every \(a_G''\)

\[
B_R^{q_R G'''} = \Pi_{q_R}^{\delta} \cdots \Pi_{q_R}^{2} B_R^{q_R} \Pi_{q_R}^{1} \cdots \Pi_{q_R}^{1}
\]

where for simplicity we wrote \(G'' = \{1, \ldots, g''\}\).

Then the success probability of the players, conditioned on the referee asking questions \((q',q)\) such that \(q'\) includes \(q_R\) in the positions in \(R\), and summed over all valid answers which include \(a_R\) for Bob, is at most

\[
(\delta + e^{-(1 - 1 - \delta)^2} \gamma) \text{Tr}(B_{q_R}^{q_R})
\]

We end this section by sketching the proof of Theorem 7 follows from the previous claims. We first set parameters: let \(C_0\) be a large enough constant, \(\varepsilon = \delta^2 C_0^{-1}\) (recall that \(\delta\) is the target value for the repeated game \(G_{FK}(\ell)\)), \(\eta = \ell/20\), and \(g = -\log(\delta(1 - s))/4\). Recall also that \(C_1\) was defined as \(C_1 = \ell/8\), and assume that \(\ell > \delta^{-200-\varepsilon}\), where \(C_2\) is the constant which appears in Claim 14.

This choice of parameters satisfies the following constraints:

- \(\varepsilon > 16C_1^{-1/2}\), which is used in Lemma 12.
- \(\eta > C_2^{-1/2}\), which is used in Claim 14 and Lemma 15.
- \(\varepsilon > C_1 C_2^{-1}\), which is used in Claim 16.

In game \(G_{FK}(\ell)\), we can think of the referee as first picking \(r^* \leq C_1/2\) pairs of questions \((R,(q_R,q_R))\) for the players, then picking \(g\) pairs \((G_1,(q_G_1,q_G_1))\), then \(C_1 - r^* - g\) pairs \((G_2,(q_G_2,q_G_2))\) and finally \(C_2\) independent pairs of confuse questions \((F,(q_F,q_F))\). Let \(G = G_1 \cup G_2\) and \((q',q) = (q_G, q_F, q_G, q_F, q_G, q_F, q_G, q_F, q_G, q_F)\). Let \(\{a_{k_{q'}}\}_{k_{q'}}\) be Alice’s POVM on question \(q'\), and \(\{B_{q_{k_{q'}}}\}\), Bob’s POVM on question \(q\).

By Lemma 12, one of two cases hold. Either a \((1 - \varepsilon)\) fraction of blocks \((R,q_R)\) are \(\varepsilon\)-dead, in which case the player’s success probability is readily bounded by \(\varepsilon + \sqrt{2\varepsilon}\) by Claim 16. Otherwise, it must be that we are in case 2 of the lemma, so that \(\varepsilon\)-alive blocks are for the most part serial. Note that any dead blocks contribute at most \(\sqrt{2\varepsilon}\) to the success probability, by Claim 16. A similar argument to that in Claim 16 shows that alive blocks which are not \((1 - \eta)\)-serial also contribute at most \(\sqrt{2\varepsilon}\), given the fact that we are in the second case of Lemma 12, and there can only be few such blocks by (4).

Suppose \((R,q_R,a_R)\) is \((1 - \eta)\)-serial. By Lemma 15, for every \((i,q_i)\) there exists a projective measurement \(\{\Pi_{g_i}^{q_i}\}_{a_i}\), depending only on \(q_R, a_R, q_i, a_i\), such that with high probability over the choice of \((G,q_G)\) such that \(g = \eta g_{\varepsilon}^{\eta}\) is a partition \(G = G'' \cup G'''\) such that \(g'' = |G''| \geq (1 - \eta^4/g)^{1/4}\) and Eq. (6) from Lemma 15 is satisfied. A small calculation (omitted) shows that this implies that the statistical distribution of outcomes produced by Alice and Bob (conditioned on Bob answering \(a_R\) to \(q_R\)) is close to that which would be obtained if Bob was to use the operators

\[
\Pi_{q_R}^\delta \cdots \Pi_{q_R}^1 B_R^{q_R} \Pi_{q_R}^1 \cdots \Pi_{q_R}^1
\]

as his POVM on questions \(q_R\). The success probability of the latter, when summed over all valid answers to the pair of questions \((q_G, q_F)\), can in turn be bounded by Claim 17.

Overall, and given our choice of parameters \(\varepsilon, \eta, \varepsilon\), and \(\ell\), it can be checked that the player’s success probability is at most \(\delta\), which proves the theorem as long as \(\ell = \text{poly}(\delta^{-1}, (1 - s)^{-1})\) is large enough.

4. APPROXIMATE BLOCK DIAGONALIZATION OF ALMOST-ORTHOGONAL OPERATORS

The orthogonalization lemma, Lemma 19 below, shows that pairwise almost-orthogonal operators are close to having a joint block-diagonal decomposition. Its proof is based on a variant of Schönenmann’s solution to the “orthogonal Procrustes” problem. Given any square matrices \(A\) and \(B\), this is the problem of finding the orthogonal matrix \(\Omega\) which minimizes

\[
\Omega := \text{argmin} \|A - B\Omega\|_F^2
\]

where \(\|X\|_F = d^{-1/2} \text{Tr}(X^\dagger X)\) is the normalized Frobenius norm. Schönenmann [28] showed that the optimal \(\Omega = \Omega = UV^\dagger\), where \(U\) and \(V\) is the singular value decomposition of \(B^T A\). Indeed, given unit vectors \(|u_1\), \ldots, \(|u_k\), one can let \(A\) be the matrix with columns the \(|u_i\), and \(B\) the identity. In this case, the orthogonal Procrustes’ problem consists in finding the best rigid rotation which maps the canonical basis of space to the vectors \(|v_j\), where the error is measured in the least squares sense — the columns of the corresponding orthogonal matrix will then form an orthonormal family close to the \(|u_i\).

We extend this method to show that it can also be carried out in the case of interest for us, that of approximately orthogonal projectors, resulting in the following.

Claim 18. Let \(P_1, \ldots, P_k\) be \(d\)-dimensional projectors such that

\[
\sum_{i \neq j} \text{Tr}(P_i P_j) \leq \varepsilon
\]

for some \(\varepsilon > 0\). Then there exists orthogonal projectors \(P_1, \ldots, P_k\) such that

\[
\sum_{i = 1}^k \text{Tr}(P_i - P_i^2)^2 = O(\varepsilon^{7/4})
\]

Note that here the difficulty is in obtaining an estimate which depends on \(\varepsilon\) only, and not on the number of projectors \(k\); this prevents the use of iterative methods “à la Gram-Schmidt”. Claim 18 is the main ingredient in the proof of the orthogonalization lemma below.

\footnote{According to Wikipedia, Procrustes, or “the stretcher”, a figure from Greek mythology, was a rogue smith and bandit from Attica who physically attacked people, stretching them, or cutting off their legs so as to make them fit an iron bed’s size.}
Lemma 19. [Orthogonalization Lemma] There is a $c > 0$ such that the following holds. Let $X_i, i = 1, \ldots, k$ be positive matrices such that

$$\sum_{i \neq j} T_{\mathcal{F}}(X_i, X_j) \leq \varepsilon \quad (7)$$

and $\sum_i X_i \leq \text{Id}$. Then there exists orthogonal projectors $\{\Pi_i\}$ such that

$$\sum_i T_{\mathcal{F}}((X_i - \Pi_i)X_i) \leq O(\varepsilon^2) \quad (8)$$

Proof. For every $i$, let $P_i$ be the projector on the span of the eigenvectors of $X_i$ with corresponding eigenvalue at least $\varepsilon/4$. Then by definition $P_i \leq \varepsilon^{-1/4} X_i$, so that (7) implies (using the positivity of $X_i$):

$$\sum_{i \neq j} T_{\mathcal{F}}(P_i, P_j) \leq \varepsilon^{1/2} \quad (8)$$

This lets us apply Claim 18 to the $P_i$, recovering orthogonal projectors $\Pi_i$ such that

$$\sum_{i = 1}^k T_{\mathcal{F}}((P_i - \Pi_i)^2) = O(\varepsilon^{1/8}) \quad (9)$$

so that we can bound

$$\sum_i T_{\mathcal{F}}((X_i - \Pi_i)X_i)^2 \leq 2 \sum_{i \neq j} \left( T_{\mathcal{F}}(X_i, X_j) + T_{\mathcal{F}}((\Pi_i X_i(\Pi_i - X_i))^2) \right)$$

$$\leq 2 \sum_{i \neq j} T_{\mathcal{F}}(\Pi_i X_i)$$

$$\leq 4 \sum_{i \neq j} T_{\mathcal{F}}(P_i X_i) + O(\varepsilon^{1/16})$$

$$= O(\varepsilon^{1/16})$$

where the second inequality uses $X_i \leq \text{Id}$, the third uses Cauchy-Schwarz, $\sum_i X_i \leq \text{Id}$, and (9), and the last uses $P_i \leq \varepsilon^{-1/4} X_j$ and the almost-orthogonality of the $P_i$ (8). \qed

5. DISCUSSION AND OPEN QUESTIONS

Our work shows for the first time that the entangled value of games can be decreased through parallel repetition. Even though we framed and proved our results in the context of 2-player games, it should not be hard to extend them in some cases to multiple players, depending on the kind of projection or consistency constraints that one can assume on the game. On the other hand, extending the result to either many-round games, or games with quantum messages, is an interesting open question.

One implication of our result is the following. The celebrated PCP theorem says that given a game, it is NP-hard to tell if its value is 1 or less than, say, 0.99. Combined with Raz’s parallel repetition result, one obtains that it is also hard to tell if the value is 1 or less than, say, 0.01. The latter statement led to an enormous body of work on strong hardness of approximation results [14]. It is currently a major open question whether an analogue of the PCP theorem holds for the entangled value. If such a result was proved, our results would allow to amplify the hardness to 1 vs. 0.01, as in the classical case, possibly leading to further surprising implications.

The main open question left by our work is whether it is possible to show a better rate of decay, in particular an exponential rate as Raz obtained from direct parallel repetition, or [17] first obtained in the setting of direct product testers. Another open question is whether our statement can be extended to hold for simple parallel repetition for arbitrary entangled games (i.e. without adding dummy or consistency questions).

We believe that our main conceptual contributions are the extension of the notion of “approximately serial” to the setting of measurements, and our subsequent orthogonalization lemma. We hope that these techniques might prove useful elsewhere, perhaps in establishing hardness of entangled games. Lastly, product testers are very useful in the area of property testing, and it remains to be seen if our result can be applied similarly.

6. ACKNOWLEDGMENTS

We are indebted to Ryan O’Donnell for making publicly available his extremely clear and helpful lecture notes [23, 22] on Feige and Kilian’s parallel repetition result, and to user “ohai” of MathOverflow.net for pointing out the connection between the classical Procrustes problem and that of the robust orthonormalization of almost-orthogonal families of vectors. We especially thank Oded Regev for useful discussions and helpful comments, and Tsuyoshi Ito and Ben Reichardt for comments.

7. REFERENCES


APPENDIX

The following useful claim is the analogue of Lemma 10 in [10], modeled after Lemma 2.1 in [22].

Claim 20. Let $C$ be an integer, and $f : Q^C \to \{X \in \mathbb{C}^{d \times d}\}$. Let $M = E_{q_1} [f(q_1)]$ and for any $(i, q_i), M_{i,q_i} = E_{q_{i+1}} [f(q_i)]$. Suppose that $E_{q_1} [\|f(q_1)\|^2] \leq 1$. Then

1. $0 \leq E_{i,q_1} [\|M - M_{i,q_i}\|^2] \leq \frac{E_{i,q_1} [\|f(q_i)\|^2]}{E_{q_1} [E_{q_{i+1}} [\|f(q_i)\|^2]]} \leq \frac{C}{2}$.
2. $E_{i,q_1} [\|M - M_{i,q_i}\|^2] = E_{q_1} [\|M_{i,q_i}\|^2] - \|M\|^2$.
3. $Pr_{i,q_1} (Tr(M) - Tr(M_{i,q_i})) \geq C^{-1/3} \leq C^{-1/3}$.

Proof. The proof of all three parts is in close analogy to that of Lemma 2.1 in [22], which shows similar statements for a Boolean function $f$. For part 1 note that

$$E_{i,q_1} [\|M - M_{i,q_i}\|^2] = \frac{1}{C} \sum_{i=1}^{C} E_{q_i} [\|M - M_{i,q_i}\|^2]$$

and hence it suffices to show that $\sum_{i=1}^{C} E_{q_i} [\|M - M_{i,q_i}\|^2] \leq Tr(M)$. Observe that

$$0 \leq E_q [\|f(q) - \sum_i (M_{i,q_i} - M)\|^2]$$

$$= E_q [\|f(q)\|^2] - \sum_i E_{q_i} [\langle M_{i,q_i} - M, M_{i,q_i} \rangle]$$

$$+ \sum_{i,j} E_{q_i,q_j} [\|M_{i,q_i} - M_{j,q_j}\|^2]$$

where for the last equality we have used that $E_q [M_{i,q_i} - M] = 0$ and hence

$$E_{q_i,q_j} [\|M_{i,q_i} - M_{j,q_j}\|^2] = 0$$

and, for $i \neq j$,

$$E_{q_i,q_j} [\langle M_{i,q_i} - M_{j,q_j}, M_{i,q_i} - M_{j,q_j} \rangle] = 0$$

Part 1 now follows, and the second inequality is simply the assumption that $E_q [\|f(q)\|^2] \leq 1$.

Part 2 is trivial from the expansion of $\|M - M_{i,q_i}\|^2$. Part 3 follows from part 1 using Markov’s inequality, which gives

$$Pr_{i,q_1} (Tr(M - M_{i,q_i}))^2 \geq C^{-2/3} \leq C^{2/3} E_{i,q_1} [Tr(M - M_{i,q_i})]^2$$

Observing that for $A := M - M_{i,q_i}$ we have $Tr(A)^2 = \langle A, Id \rangle^2 \leq \|A\|^2, \|Id\|^2 = \|A\|^2$ gives the desired bound. □